



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/758,852

01/16/2004

Frank J. Hammond II

413127

6951

30955 7590 06/04/2007
LATHROP & GAGE LC
4845 PEARL EAST CIRCLE
SUITE 300
BOULDER, CO 80301

EXAMINER

TRAN, ELLEN C

ART UNIT

PAPER NUMBER

2134

MAIL DATE

DELIVERY MODE

06/04/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/758,852

Applicant(s)

HAMMOND ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

1. This action is responsive to: amendment filed original application filed on 16 January 2004 with acknowledgement of the benefit of a provisional application filed 16 January 2003.
2. Claims 1-19 are pending; claims 1, 14, 15, and 18, are independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 15-19**, are rejected under 35 U.S.C. 102(e) as being anticipated by Lee et al. U.S. Patent Application Publication No. 2004/0015719 (hereinafter '719).

As to independent claim 15. A system for event monitoring, comprising: an electronic network for collecting events” is taught in '719 page 1, paragraph 0013;

“one or more event correlation engines, each event correlation engine being connected to the electronic network and having a receive event handler for receiving events addressed to the event correlation engine; and one or more event correlation modules, each of the event correlation modules having an event pattern that defines events of interest” is shown in '719 page 1, paragraph 0014;

“each of the correlation modules receiving all events received by the event correlation engine, the event correlation module correlating the events of interest” is disclosed in ‘719 page 1, paragraph 0015.

As to dependent claim 16, **“wherein the event correlation module is a simulated annealing correlator module”** is taught in ‘719 pages 1-2, paragraph 0016 (annealing equates to learning if new attack pattern determined).

As to dependent claim 17, **“the simulated annealing correlator further comprising: recorded events; a simulated annealing correlator engine; heuristics; and a correlation threshold; wherein the simulated annealing correlator engine utilizes the heuristics and the correlation threshold to correlate the events received by the event correlation engine with the recorded events, the correlated events being added to the recorded events”** is shown in ‘719 page 4, paragraph 0053.

As to independent claim 18, **“A method of pattern recognition, comprising: collecting electronic network events; sampling the electronic network events with one or more event correlation engines”** is taught in ‘719 page 1, paragraphs 0013;

“passing sampled electronic network events from each event correlation engine to one or more event correlator modules within each event correlation engine; comparing events in each of the event correlator modules by sampling the events, determining if any of the events matches an event pattern, and, if there is a match, creating a new event announcing the match and passing the new event to the associated event correlation engine for electronic network distribution” is shown in ‘719 page 1, paragraph 0014;

Art Unit: 2134

“and determining patterns in events using a simulated annealing correlator, determining if the pattern is important, and, if so, creating a new event announcing the important pattern and passing the new event to the associated event correlation engine for network distribution” is disclosed in ‘719 page 1, paragraphs 0015-0016.

As to dependent claim 19, “wherein the step of sampling further comprises sampling all of, or less than all of, the electronic network events” is taught in ‘719 page 3, paragraph 0039.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 1-9**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. U.S. Patent Application Publication No. 2004/0015719 (hereinafter ‘719) in view of Ghosh et al. U.S. Patent No. 7,181,768 (hereinafter ‘768).

As to independent claim 1, “A method of protecting an electronic network, comprising: installing one or more agents within components of the electronic network” is taught in ‘719 page 3, paragraph 0040;

Art Unit: 2134

“monitoring the electronic network for abnormal activity using the agents; and protecting the electronic network by blocking the abnormal activity using the agents” ‘is shown in ‘719 page 1, paragraph 0014;

the following is not explicitly taught in ‘719: **“performing an initial assessment of the electronic network to determine normal activity”** however ‘768 teaches that the present invention uses ‘machine learning’ for an intrusion detection system in col. 4, lines 40-44, which is defined in col. 2, lines 10-24 as defining normal behavior in anomaly detection by first building user profiles based on the sequence of each user’s normal command executions.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of an intelligent security engine and system taught in ‘012 to utilize machine learning anomaly detection. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to utilize learning anomaly detection in an application-based intrusion detection system see ‘768 (col. 4, lines 25 et seq.) “As discussed previously, prior IDSs have employed neural networks to build user profiles based on sequences of commands entered by users. These user-based IDSs were implemented using feed-forward multi-layer perceptron networks, also known as "backpropagation neural networks" or simply "backprops." The backprop is trained to recognize patterns of normal user behavior. After the training, the backprop is used to identify intruders based on deviations from the established user patterns. However, because of the complexities in establishing adequate learning criteria and other problems discussed herein, neural networks have heretofore not been implemented in application-based intrusion detection systems”.

As to dependent claim 2, “wherein the step of installing comprises the step of installing a type 2 super peer agent for authorizing and reauthorizing the agents” is disclosed in ‘719 on page 4, paragraphs 0049-51.

As to dependent claim 3, “further comprising logically connecting at least one of the agents into one or more cooperative agent cells” is taught in ‘719 on page 3, paragraph 0039.

As to dependent claim 4, “wherein the step of installing further comprises: establishing bidirectional communication protocols for agent communication within the cooperative agent cells; delegating one or more agents in the cooperative agent cells to have bidirectional communication with another delegated agent; and establishing bidirectional communication protocols for each delegated agent to communicate with another delegated agent” is taught in ‘719 page 4, paragraph 0056:

As to dependent claim 5, “wherein the step of installing further comprises: broadcasting a request for agents to submit to authentication; and authenticating submitted agents” is shown in ‘719 page 4, paragraph 0056.

As to dependent claim 6, “wherein the step of logically connecting further comprises self-organizing at least one of the agents into each of the cooperative agent cells” is disclosed in ‘719 page 3, paragraphs 0040-0041.

As to dependent claim 7, “wherein the step of establishing further comprising communicating via at least one covert communication protocol” is taught in ‘719 page 4, paragraph 0056.

As to dependent claim 8, “wherein the step of performing an initial assessment comprises: mapping systems, communication ports and attached devices of the electronic

Art Unit: 2134

network; and establishing normal activity of the systems, communication ports, and attached devices” is shown in ‘719 page 5, paragraph 0064-0065.

As to dependent claim 9, “wherein the step of monitoring comprises: non-destructively intercepting communications on the electronic network; collecting events from the intercepted communications; and determining if the events indicate abnormal activity” is shown in ‘719 on page 1, paragraph 0013.

7. **Claims 10 and 14**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. U.S. Patent Application Publication No. 2004/0015719 (hereinafter ‘719) in view of Ghosh et al. U.S. Patent No. 7,181,768 (hereinafter ‘768) in further view of Ghosh et al. U.S. Patent No. 7,181,768 (hereinafter ‘768).

As to independent claim 14, “A system for protecting an electronic network, comprising: a plurality of agents with the electronic network, the agents being grouped into at least one cooperative agent cell having one cell delegate” is taught in ‘719 page 3, paragraph 0040;

“a communications protocol within each cooperative agent cell, for (a) communicating between agents of the cooperative agent cell, and (b) communicating with cell delegates external to the cooperative agent cell” is taught in ‘719 page 4, paragraph 0056; **“means for detecting malicious activity”** is shown in ‘719 page 3, paragraph 0041;

“means for counter-intelligence to reveal the origin of the malicious activity” is disclosed in ‘719 page 4, paragraph 0051;

the following is not explicitly taught in ‘719: **“means for determining normal activity levels of the electronic network”** however ‘768 teaches that the present invention uses ‘machine

Art Unit: 2134

learning' for an intrusion detection system in col. 4, lines 40-44, which is defined in col. 2, lines 10-24 as defining normal behavior in anomaly detection by first building user profiles based on the sequence of each user's normal command executions;

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of an intelligent security engine and system taught in '012 to utilize machine learning anomaly detection. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to utilize learning anomaly detection in an application-based intrusion detection system see '768 (col. 4, lines 25 et seq.) "As discussed previously, prior IDSs have employed neural networks to build user profiles based on sequences of commands entered by users. These user-based IDSs were implemented using feed-forward multi-layer perceptron networks, also known as "backpropagation neural networks" or simply "backprops." The backprop is trained to recognize patterns of normal user behavior. After the training, the backprop is used to identify intruders based on deviations from the established user patterns. However, because of the complexities in establishing adequate learning criteria and other problems discussed herein, neural networks have heretofore not been implemented in application-based intrusion detection systems".

the following is not explicitly taught in '719:

"means for isolating compromised components of the electronic network" however '936 teaches that the system includes a trap system create a virtual cage in col. 7, lines 42-51;

"means for repairing damage caused by the malicious activity; means for determining vulnerabilities in the current protection provided by the plurality of agents; and means for improving protection to resist future attack on the electronic network"

Art Unit: 2134

however '936 teaches "The inventive system focuses on discovering and presenting information about an attack, and presents configuration problems that are likely related to the attack, while suppressing those that aren't. Additionally, the presentation may show where relevant configuration problems fit within the factors that made the attack possible. This facilitates recovering from the attack, because the system administrator may be able to block future attacks of the same type by fixing only a subset of factors involved rather than having to fix every possible factor. It is also extremely useful in situations where one of the configuration problems cannot be changed due to its providing crucial functionality for the enterprise. For example, the restore command should normally not be set to allow execution by normal users with SetUID to root because it can be used to allow a normal user to install his own SetUID program on the computer that gives him a root shell. However, the dump-restore command pair have features that make them preferable in various circumstances to the other commonly available archiving and file copying utilities, and thus a system administrator may decide that having this capability available is worth the security risk" in col. 12, lines 9-29.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of an intelligent security engine and system that includes a machine learning anomaly taught in '012 and '768 to include a mechanism to quarantine attacked systems. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to improve existing intrusion detection systems see '936 (col. 3, lines 3 et seq.) "The third dimension is real-time or after-the-fact. All conventional IDSes fall into the real-time category: their intention is to alert the operator to an attack so that he can respond in time to avert damage. However, the speed with which attacks are currently executed

Art Unit: 2134

rarely allow time for any meaningful response from these systems. The after-the-fact category is dominated by forensic tools: utilities designed to help a computer security expert analyze what happened on a compromised host by extracting data that has been established as relevant to known attacks. The exception to this is the DERBI project (Diagnosis, Explanation and Recovery from Break-Ins), which experimented with the feasibility of after-the-fact detection of intrusions on hosts with no special data collection enabled. The DERBI project developed a loosely coupled system that processed data for a single known simulated host in an experimental testbed. The existing systems, however, have many limitations: they fail to utilize many useful sources of data, they produce large amounts of information that are difficult for a human to analyze in a timely fashion, they are complex and difficult to use, and they are often designed for system administration rather than attack diagnosis”.

As to **dependent claim 10**, the following is not explicitly taught in the combination of teaching of ‘719 and ‘768: **“wherein the step of protecting comprises one or more of: luring a malicious agent that causes abnormal activity into a false appearance of success; planting instructions on information retrieved by the malicious agent to assist in identifying the origins of the malicious agent”** however ‘936 teaches that the system includes a trap system create a virtual cage in col. 7, lines 42-51;

“isolating electronic network components which have been compromised by the malicious agent; attacking the malicious agent; formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network; installing patches to eliminate vulnerabilities in the electronic network; reassessing the electronic network to detect

abnormal operations; and investigating abnormal operations of the electronic network”

however ‘936 teaches “The inventive system focuses on discovering and presenting information about an attack, and presents configuration problems that are likely related to the attack, while suppressing those that aren’t. Additionally, the presentation may show where relevant configuration problems fit within the factors that made the attack possible. This facilitates recovering from the attack, because the system administrator may be able to block future attacks of the same type by fixing only a subset of factors involved rather than having to fix every possible factor. It is also extremely useful in situations where one of the configuration problems cannot be changed due to its providing crucial functionality for the enterprise. For example, the restore command should normally not be set to allow execution by normal users with SetUID to root because it can be used to allow a normal user to install his own SetUID program on the computer that gives him a root shell. However, the dump-restore command pair have features that make them preferable in various circumstances to the other commonly available archiving and file copying utilities, and thus a system administrator may decide that having this capability available is worth the security risk” in col. 12, lines 9-29.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of an intelligent security engine and system that includes a machine learning anomaly taught in ‘012 and ‘768 to include a mechanism to quarantine attacked systems. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to improve existing intrusion detection systems see ‘936 (col. 3, lines 3 et seq.) “The third dimension is real-time or after-the-fact. All conventional IDSes fall into the real-time category: their intention is to alert the operator to an attack so that he can

Art Unit: 2134

respond in time to avert damage. However, the speed with which attacks are currently executed rarely allow time for any meaningful response from these systems. The after-the-fact category is dominated by forensic tools: utilities designed to help a computer security expert analyze what happened on a compromised host by extracting data that has been established as relevant to known attacks. The exception to this is the DERBI project (Diagnosis, Explanation and Recovery from Break-Ins), which experimented with the feasibility of after-the-fact detection of intrusions on hosts with no special data collection enabled. The DERBI project developed a loosely coupled system that processed data for a single known simulated host in an experimental testbed. The existing systems, however, have many limitations: they fail to utilize many useful sources of data, they produce large amounts of information that are difficult for a human to analyze in a timely fashion, they are complex and difficult to use, and they are often designed for system administration rather than attack diagnosis”.

8. **Claims 11-13**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al. U.S. Patent Application Publication No. 2004/0015719 (hereinafter ‘719) in view of Ghosh et al. U.S. Patent No. 7,181,768 (hereinafter ‘768) in further view of Rowland et al. U.S. Patent No. 7,058,968 (hereinafter ‘968).

As to dependent claim 11, the following is not explicitly taught in the combination of teaching of ‘719 and ‘768: **“further comprising promoting one of the agents in each of the cooperative agent cells to a cell delegate”** however ‘968 teaches that the architecture of the system is designed to allow modularity. This modularity allows for the roles to be reversed. In col. 4, lines 44-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of an intelligent security engine and system that utilizes machine learning anomaly detection taught in '012 and '719 to include a means to develop a hierarchical agent installation promoting agents. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to allow for flexibility for mobile autonomous agents see '968 (col. 1, lines 58 et seq.) "It is desirable to provide a computer security and management system that enables a distributed framework for command, control and communication that enables systems, devices and operational personnel to interact with a network as a unified entity. It is further desirable to provide this command, control and communication by using a core communication architecture that allows local and remote execution of mobile program code, and static execution of program code. Such a system should enable flexible communication formats, self-healing network techniques, and expansion by adding new program modules, software handlers, and mobile autonomous agents".

As to dependent claim 12, "further comprising: promoting a second agent in each of the cooperative agent cells to a type 1 super peer agent; authenticating new agents with the type 1 super peer agent; and communicating between the cooperative agent cells and a command and control console via the cell delegate to protect the network from malicious activity" is shown in '719 page 4, paragraph 0056.

As to dependent claim 13, "the agents and cooperative agent cells being configured for independent and collaborative investigation of the electronic network, isolation of compromised components of the electronic network, and defense of the electronic network" is taught in '719 page 3, paragraph 0040.

Art Unit: 2134

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ellen Tran
Patent Examiner
Technology Center 2134
25 May 2007